مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

MoonPeak Malware Threat

Tracking #:432316178

Date:23-08-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed researchers identified sophisticated malware infrastructure associated with a North Korean threat actor group, referred to as UAT-5394, which has developed a new variant of remote access trojan (RAT) known as MoonPeak.

TECHNICAL DETAILS:

Cisco Talos has identified a sophisticated malware infrastructure associated with a North Korean threat actor group, referred to as UAT-5394, which has developed a new variant of remote access trojan (RAT) known as MoonPeak. This malware demonstrates advanced capabilities, including evasion techniques and dynamic command and control (C2) mechanisms.

Key Points:

- MoonPeak Malware: MoonPeak is a variant of the XenoRAT malware, which has been actively developed by UAT-5394. This RAT is used for staging, command and control (C2) servers, and testing machines, indicating a high level of sophistication and operational capability.
- Infrastructure Pivoting: The threat actors are known to pivot across different C2s and staging servers to set up new infrastructure and modify existing servers. This suggests a dynamic and adaptive approach to their operations, making it harder for defenders to track and mitigate their activities.
- Links to Kimsuky: While there are overlaps in Tactics, Techniques, and Procedures (TTPs) and infrastructure patterns with the North Korean state-sponsored group Kimsuky, there is not yet substantial technical evidence to conclusively link this campaign with the APT. This raises the possibility that UAT-5394 could be a sub-group within Kimsuky or another group within the North Korean APT machinery that borrows their TTPs and infrastructure patterns.
- QuasarRAT to MoonPeak Transition: The observation that UAT-5394 has been setting up and operating QuasarRAT C2 servers before adopting XenoRAT and MoonPeak suggests a strategic shift in their toolset. This could indicate a move towards more advanced or tailored malware capabilities.
- Testing and Staging Infrastructure: Cisco Talos has uncovered the infrastructure used to create new iterations of MoonPeak. The C2 server hosts malicious artifacts for download and is used to access and set up new infrastructure to support the campaign. The threat actors also update their payloads and retrieve logs from infected systems, showing a continuous cycle of development and operational refinement.
- Access via VPN Nodes: The use of VPN nodes to access their infrastructure adds an extra layer of complexity to their operations, making it more challenging for security analysts to trace their activities back to their origin.
- Implications for Defense: Organizations should be aware of the evolving threat landscape and the capabilities of state-sponsored actors like UAT-5394. This includes staying informed about new malware variants, understanding the TTPs of these groups, and implementing robust security measures to detect and respond to such threats.

Indicators of Compromise:
Attached File

RECOMMENDATIONS:

- Implement advanced threat detection systems that can identify unusual network traffic patterns, especially those indicative of C2 communications.
- Regularly update and fine-tune intrusion detection and prevention systems (IDPS) to recognize signatures associated with MoonPeak and similar malware.
- Perform comprehensive security assessments to identify vulnerabilities within your network and systems.
- Ensure that all software, especially remote access tools, is up to date with the latest security patches.
- Conduct training sessions for employees to recognize phishing attempts and other social engineering tactics that could lead to malware infections.
- Promote a culture of cybersecurity awareness to encourage reporting of suspicious activities.
- Segment critical systems and sensitive data to limit the lateral movement of potential intruders.
- Utilize firewalls to restrict access to and from segments where sensitive data is stored.
- Regularly back up critical data and systems to ensure rapid recovery in the event of a malware attack.
- Test backup and recovery procedures to ensure they are effective and can be executed quickly.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/